AO 106 (Rev. 06/09) Application for a Search Warrant



# UNITED STATES DISTRICT COURT

for the

Northern District of Oklahoma

In the Matter of the Search of

1403 Archer Drive, Claremore, Oklahoma

Case No. 19-MJ-232-JFJ

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property:

See Attachment "A"

located in the Northern District of Oklahoma, there is now concealed:

See Attachment "B"

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

| *Code Section* | *Offense Description* |
|---|---|
| **18 U.S.C. § 2252(a)(2)(A)** | **Distribution of Child Pornography** |
| **18 U.S.C. § 2252(a)(5)(B)** | **Possession of and access with intent to view child pornography** |

The application is based on these facts:

**See Affidavit of Dustin L. Carder, SA HSI, attached hereto.**

☑ Continued on the attached sheet.

☐ Delayed notice of ___ days (give exact ending date if more than 30 _____ ) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

*Applicant's signature*

Dustin L. Carder, SA HSI

*Printed name and title*

Sworn to before me and signed in my presence.

Date: 11-5-19

*Judge's signature*

City and state: Tulsa, OK Tulsa, Oklahoma

Jodi F. Jayne, U.S. Magistrate Judge

*Printed name and title*

# AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Dustin L. Carder, a Special Agent with Homeland Security Investigations (HSI), being duly sworn, depose and state as follows:

## INTRODUCTION

1. I have been employed as a Special Agent (SA) with the U.S. Department of Homeland Security (DHS), Homeland Security Investigations (HSI) since December 2018, and am currently assigned to the Office of the Resident Agent in Charge in Tulsa, Oklahoma. While employed by HSI, I have investigated federal criminal violations related to high technology or cybercrime, child exploitation, and child pornography. I have gained experience through training at the sixteen-week Homeland Security Investigations Special Agent Training (HSISAT) program, working with more experienced investigators, and everyday work relating to conducting these types of investigations. I have received training in the area of child pornography and child exploitation and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media including computer media. Moreover, I am a federal law enforcement officer who is engaged in enforcing the criminal laws, including 18 U.S.C. §§ 2251, 2252, and 2252A, and I am authorized by law to request a search warrant.

2. This affidavit is submitted in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant for the locations specifically described in **Attachment A** of this Affidavit including the entire property located at **1403 Archer Drive, Claremore, Oklahoma** (herein after known as the "SUBJECT PREMISES"), the content of

electronic storage devices located therein, and any person located at the SUBJECT PREMISES, for contraband and evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 2252A(a)(2)(A) (distribution of child pornography); and 18 U.S.C. §§ 2252A(a)(5)(B) (possession of and access with intent to view child pornography), which items are more specifically described in **Attachment B** of this Affidavit.

3. The statements in this affidavit are based in part on information provided by other law enforcement officers and on my investigation of this matter. Since this Affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that contraband and evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 2252A(a)(2)(A) (distribution of child pornography); and 18 U.S.C. §§ 2252A(a)(5)(B) (possession of and access with intent to view child pornography), are presently located at the SUBJECT PREMISES.

## STATUTORY AUTHORITY

4. As noted above, this investigation concerns alleged violations of the following:

a. Title 18, United States Code, Sections 2252A(a)(2)(A) prohibits a person from knowingly receiving or distributing, or attempting or conspiring to receive or distribute, any child pornography or any material that contains child pornography, as defined in 18 U.S.C. § 2256(8), that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

b. Title 18, United States Code, Sections 2252A(a)(5)(B) prohibits a person from knowingly possessing or knowingly accessing with intent to view, or attempting or conspiring to do so, any material that contains an image of child pornography, as defined in 18 U.S.C. § 2256(8), that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce, or in or affecting interstate or foreign commerce, by any means, including by computer, or that was produced using materials that have been mailed or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

## DEFINITIONS

5. The following definitions apply to this Affidavit and Attachment B:

a. "Chat," as used herein, refers to any kind of text communication over the Internet that is transmitted in real-time from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a format that resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and email.

b. "Chat room," as used herein, refers to the ability of individuals to meet in one location on the Internet in order to communicate electronically in real-time to other individuals. Individuals may also have the ability to transmit electronic files to other individuals within the chat room.

c. "Child erotica," as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily obscene or do not necessarily depict minors engaging in sexually explicit conduct.

d. "Child pornography," as defined in 18 U.S.C. § 2256(8), is any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical or other means, of sexually explicit conduct, where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

e. A "communication port" is an endpoint of communication in an operating system. A port is always associated with an IP address of a host and the protocol type of the communication. Specific port numbers are often used to identify specific services.

f. "Computer," as used herein, refers to "an electronic, magnetic, optical, electrochemical, or other high-speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device" and includes smartphones, and mobile phones and devices. *See* 18 U.S.C. § 1030(e)(1).

g. "Computer hardware," as used herein, consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes,

and other memory storage devices); peripheral input/output devices (including keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including physical keys and locks).

h. "Computer passwords and data security devices," as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates what might be termed a digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

i. "Hyperlink" refers to an item on a web page which, when selected, transfers the user directly to another location in a hypertext document or to some other web page.

j. "Hyper Text Markup Language," or "HTML," as used herein, is a standard protocol for formatting and displaying documents, such as web pages, on the Internet.

k. An "Internet Protocol address" or "IP address," as used herein, refers to a unique number used by a computer or other digital device to access the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer or device accessing the Internet must be assigned

an IP address so that Internet traffic sent from and directed to that computer or device may be directed properly from its source to its destination. Most Internet service providers (ISPs) control a range of IP addresses. IP addresses can be "dynamic," meaning that the ISP assigns a different unique number to a computer or device every time it accesses the Internet. IP addresses might also be "static," if an ISP assigns a user's computer a particular IP address that is used each time the computer accesses the Internet. ISPs typically maintain logs of the subscribers to whom IP addresses are assigned on particular dates and times.

l. "Internet Service Providers" ("ISPs"), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment.

m. The "Internet" is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

n. "Minor," as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

o. "Records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

p. "Remote Computing Service" ("RCS"), as defined in 18 U.S.C. § 2711(2), is the provision to the public of computer storage or processing services by means of an electronic communications system.

q. "Sexually explicit conduct," as defined in 18 U.S.C. § 2256(2), means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person.

r. A "storage medium" is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

s. "Visual depiction," as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

## BACKGROUND ON KIK AND KIK REPORTS

6. Kik Messenger (hereinafter "Kik") is a mobile application designed for chatting or messaging owned and operated by Kik Interactive, Inc. According to the publicly available

document "Kik's Guide for Law Enforcement,"[1] to use this application, a user downloads the application to a mobile phone, computer, or other digital device via a service such as the iOS App Store, Google Play Store, Apple iTunes, or another similar provider. Once the application is downloaded and installed, the user is prompted to create an account and username. The user also creates a display name, which is a name that other users see when transmitting messages back and forth. Once the user has created an account, the user is able to locate other users via a search feature. While messaging, users can then send each other text messages, images, and videos.

7. According to "Kik's Guide for Law Enforcement," Kik users are also able to create chat groups with a limited number of individuals to communicate in a group setting and exchange text messages, images and videos. These groups are administered by the group creator who has the authority to remove and ban other users from the created group. Once the group is created, Kik users have the option of sharing a link to the group that includes all of their contacts or any other user. These groups are frequently created with a group name containing a hashtag (#) that is easily identifiable or searchable by keyword.

8. According to information provided to HSI by a Kik Law Enforcement Response Team Lead, Kik's Terms of Service prohibit Kik users from uploading, posting, sending, commenting on, or storing content that contains child pornography and/or child abuse images. The Terms of Service also provide that Kik may review, screen and delete user content at any time if Kik believes use of their services are in violation of the law. According to Kik, Kik has a strong business interest in enforcing their Terms of Service and ensuring that their services are free of

[1] Available at: https://lawenforcement.kik.com/hc/en-us/categories/200320809-Guide-for-Law-Enforcement.

illegal content, and in particular, child sexual abuse material. Accordingly, Kik reports that it independently and voluntarily takes steps to monitor and safeguard their platform and that ridding Kik products and services of child abuse images is critically important to protecting their users, product, brand, and business interests.

9. Kik is located in Ontario, Canada and is governed by Canadian law. According to information contained in the "Kik Interactive, Inc. Child Sexual Abuse and Illegal Material Report and Glossary" (hereinafter Kik Glossary), which Kik provides when reporting information to law enforcement authorities, Kik is mandated to report to the Royal Canadian Mounted Police (RCMP) any images and/or videos that would constitute suspected child pornography under Canadian law which are discovered on the Kik platform. According to the Kik Glossary, Kik is typically alerted to suspected child pornography on Kik based on digital hash value matches to previously identified child pornography or through reports from other Kik users or third-party moderators.

10. The RCMP has advised Homeland Security Investigations (HSI) agents that upon receiving a report from Kik related to suspected child pornography, the RCMP reviews the reported IP addresses of the Kik users contained in the Kik Reports to determine their location. The RCMP then provides Kik Reports of Kik users in the United States to HSI in Ottawa, Canada, who in turn provides the Kik Reports to the HSI Cyber Crimes Center (C3) Child Exploitation Investigations Unit (CEIU) located in Fairfax, Virginia for analysis and dissemination.

## PROBABLE CAUSE

11. I have reviewed a Kik Report dated March 4, 2019. A review of the Kik Report shows that on March 4, 2019 at 10:03:35 UTC, a Kik user with username "spunducky0420_5o0" who provided the name "Spunducky Beester," email address "icesk8tes@gmail.com," date of birth

"July 28, 1980," who was using a Samsung SM-J337T model cellular phone, used Kik to send an image of child pornography as described herein.

12. I have learned that Kik was alerted to the child pornography through use of Microsoft's PhotoDNA technology. According to the Kik Glossary, Kik uses PhotoDNA to automatically scan user-uploaded files in order to flag images that may depict suspected child pornography and prevent such images from continuing to circulate through their application. When PhotoDNA detects a suspected child pornography file, it creates a Report and sends it to the Kik Law Enforcement team. According to information provided by a Kik Law Enforcement Response Team Lead, all suspected child pornography images and videos reported via a PhotoDNA Report, as well as any related user communications, are visually reviewed by a member of the Kik Law Enforcement Response team before a report is forwarded to law enforcement authorities. Kik trains employees comprising its Law Enforcement Response team on the legal obligation to report apparent child pornography. The Team is trained on the Canadian statutory definition of child pornography and how to recognize it on Kik products and services. Kik voluntarily makes reports to law enforcement in accordance with that training. After Kik discovered the suspected child pornography, Kik removed the content from its communications system and closed the user's account.

13. Along with Kik's Report, Kik provided a copy of the suspected child pornography image that they located to the RCMP. On October 2, 2019, I reviewed the very same image that Kik had provided with the Kik Report sent to the RCMP and forwarded to HSI. The image had previously been located, isolated, searched and viewed by Kik personnel before it was reported to the RCMP. I reviewed only the image previously located, isolated, searched and viewed by Kik

personnel and observed that the image is child pornography as defined by Federal Law. Specifically, the image distributed by the Kik username "spunducky0420_5o0" included the following:

a. The image is of a prepubescent white female with long brown hair (hereafter "victim"). The victim is wearing makeup and lipstick on her face and what appears to be a gold necklace. The victim is fully nude laying on a giraffe-type print sheet next to a cheetah-type blanket. The victim has no breast development and no visible pubic hair. The victim is holding her left leg in the air with her left arm, while her right leg is spread, fully exposing her vagina and partially exposing her anus. The image was uploaded to an undisclosed chat room within Kik on March 4, 2019 at 10:03:35 UTC.

14. The information provided by Kik included IP addresses associated with access to the pertinent Kik user account. Specifically, IP address 68.13.236.123 was used by username "spunducky0420_5o0" on March 4, 2019, to send a child pornography image. In addition, IP address 68.13.236.123 was used to access the Kik user account during the same month the Kik user sent child pornography.

15. A query of the American Registry for Internet Numbers (ARIN) online database revealed that IP address 68.13.236.123 used on March 4, 2019 to send a child pornography image was registered to Cox Communications. In addition, the IP address 68.13.236.123 used to access the Kik user account during the month the Kik user sent a child pornography image was also registered to Cox Communications.

16. On July 22, 2019, an administrative summons was sent to Cox Communications regarding the IP address described in Paragraphs 14-15. A review of the results obtained on

August 29, 2019 identified the following account holder and address, which is the address of the SUBJECT PREMISES: Kathy MCELROY at 1403 Archer Drive, Claremore, Oklahoma.

17. A search of law enforcement databases that provides names, dates of birth, addresses, associates, telephone numbers, and other information was conducted for the SUBJECT PREMISES. These queries revealed the following individuals may live at the residence: Kathy MCELROY (DOB: 06/14/1949), Virginia SMITH (aka BURT/LOPEZ) (DOB: 08/19/1976), Dakota BURT (DOB: 04/15/2000), Dalton BURT (DOB: 04/27/1997), Patricia SMITH (DOB: 04/21/2004), and Cherokee BURT (DOB 01/13/2003).

18. Surveillance of the SUBJECT PREMISES on or about October 16, 2019 revealed that a gray colored 2014 Ford Fiesta bearing Oklahoma license plate HTM-015 was parked in the driveway. A check with the Oklahoma Tax Commission via the National Law Enforcement Telecommunication System (NLETS) showed the vehicle registered to Kathy MCELROY or Virginia BURT at the SUBJECT PREMISES.

19. On or about October 22, 2019, I used a wireless device in an effort to gain additional information regarding/detect any potential wireless networks at the SUBJECT PREMISES. Positioned across the street from the SUBJECT PREMISES, I noted that there was one wireless network in the area, but it was secured. Accordingly, to use the network to access the Internet, a user would likely have to know the encryption key or password for that particular network. Based on the signal strength of the wireless network, as well as my training and experience and information relayed to me by agents, I believe that the wireless router at the SUBJECT PREMISES is likely generating a secured wireless network. As explained above, I know, from my training and experience and information relayed to me by agents, that wireless routers for both secured and

unsecured wireless networks may yield significant evidence of, or serve as instrumentalities of, a crime.

## BACKGROUND ON CHILD PORNOGRAPHY, COMPUTERS, AND THE INTERNET

20. I have had both training and experience in the investigation of computer-related crimes. Based on my training, experience, and knowledge, I know the following:

a. Computers and digital technology are the primary way in which individuals interested in child pornography interact with each other. Computers basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

b. Digital cameras and smartphones with cameras save photographs or videos as a digital file that can be directly transferred to a computer by connecting the camera or smartphone to the computer, using a cable or via wireless connections such as "WiFi" or "Bluetooth." Photos and videos taken on a digital camera or smartphone may be stored on a removable memory card in the camera or smartphone. These memory cards are often large enough to store thousands of high-resolution photographs or videos.

c. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Mobile devices such as smartphones and tablet computers may also connect to other computers via wireless connections. Electronic contact can be made to literally millions of computers around the world. Child pornography can therefore be easily, inexpensively and anonymously

(through electronic communications) produced, distributed, and received by anyone with access to a computer or smartphone.

d. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. Electronic storage media of various types – to include computer hard drives, external hard drives, CDs, DVDs, and "thumb," "jump," or "flash" drives, which are very small devices which are plugged into a port on the computer – can store thousands of images or videos at very high resolution. It is extremely easy for an individual to take a photo or a video with a digital camera or camera-bearing smartphone, upload that photo or video to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices. Some media storage devices can easily be concealed and carried on an individual's person. Smartphones and/or mobile phones are also often carried on an individual's person.

e. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

f. Individuals also use online resources to retrieve and store child pornography. Some online services allow a user to set up an account with a remote computing service that may provide e-mail services and/or electronic storage of computer files in any variety of formats. A user can set up an online storage account (sometimes referred to as "cloud" storage) from any computer or smartphone with access to the Internet. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer, smartphone or external media in most cases.

g. A growing phenomenon related to smartphones and other mobile computing devices is the use of mobile applications, also referred to as "apps." Apps consist of software downloaded onto mobile devices that enable users to perform a variety of tasks – such as engaging in online chat, sharing digital files, reading a book, or playing a game – on a mobile device. Individuals commonly use such apps to receive, store, distribute, and advertise child pornography, to interact directly with other like-minded offenders or with potential minor victims, and to access cloud-storage services where child pornography may be stored.

h. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional (*i.e.*, by saving an e-mail as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files). Digital information can also be retained unintentionally such as the traces of the path of an electronic communication may be automatically stored in many places (*e.g.*, temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

## CHARACTERISTICS COMMON TO INDIVIDUALS WHO DISTRIBUTE, RECEIVE, POSSESS, AND/OR ACCESS WITH INTENT TO VIEW CHILD PORNOGRAPHY

21. Based on my previous investigative experience related to child exploitation investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals who distribute, receive, possess, and/or access with intent to view child pornography:

a. Such individuals may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media, or from literature describing such activity.

b. Such individuals may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Such individuals almost always possess and maintain digital or electronic files of child pornographic material, that is, their pictures, videos, photographs, correspondence, mailing lists, etc., in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children typically retain pictures, videos, photographs, correspondence, and mailing lists for many years.

d. Likewise, such individuals often maintain their child pornography images in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These child pornography images are often maintained for several years and are kept close by, usually at the possessor's residence, inside the possessor's vehicle, or, at times, on their person, to enable the individual to view the child pornography images, which are valued highly. Some of these individuals also have been found to download, view, and then delete child pornography on their computers or digital devices on a cyclical and repetitive basis.

e. Such individuals may also take it upon themselves to create their own child pornography or child erotica images, videos or other recordings. These images, videos or other recordings may be taken or recorded covertly, such as with a hidden camera in a bathroom, or the individual may have child victims he or she is abusing in order to produce child pornographic or child erotica images, videos or other recordings. These images, videos or other recordings are often collected, traded, or shared.

f. Importantly, evidence of such activity, including deleted child pornography, often can be located on these individuals' computers and digital devices through the use of forensic tools. Indeed, the very nature of electronic storage means that evidence of the crime is often still discoverable for extended periods of time even after the individual "deleted" it.

g. Such individuals also may correspond with and/or meet others to share information and materials, rarely destroy correspondence from other child pornography distributors/possessors, conceal such correspondence as they do their sexually explicit

material, and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

h. Such individuals prefer not to be without their child pornography for any prolonged period of time. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world. Thus, even if "spunducky0420_5o0" uses a portable device (such as a mobile phone) to access the internet and child pornography, it is more likely than not that evidence of this access will be found in his/her home, the SUBJECT PREMISES as set forth in Attachment A.

22. As detailed herein, the Kik user "spunducky0420_5o0" distributed child pornography via Kik. In order to distribute such material, the user would necessarily have to acquire and possess child pornography.

**SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS**

23. As described above and in Attachment B, this application seeks permission to search for records that might be found on the SUBJECT PREMISES, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media, such as a cellular phone or tablet. Thus, the warrants applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

24. I submit that if a computer or storage medium is found on the SUBJECT PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence,

because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

25. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrants, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the SUBJECT PREMISES because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when,

where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In your affiant's training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image

was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

f. I know that when an individual uses a computer to obtain or access child pornography, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

26. Based upon my training and experience and information relayed to me by agents and others involved in the forensic examination of computers, I know that computer data can be stored on a variety of systems and storage devices, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact disks, magnetic tapes, memory cards, memory chips, and online or offsite storage servers maintained by corporations, including but not limited to "cloud" storage. I also know that during the search of the premises it is not always

possible to search computer equipment and storage devices for data for a number of reasons, including the following:

a. Searching computer systems is a highly technical process which requires specific expertise and specialized equipment. There are so many types of computer hardware and software in use today that it is impossible to bring to the search site all of the technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may also be necessary to consult with computer personnel who have specific expertise in the type of computer, software website, or operating system that is being searched;

b. Searching computer systems requires the use of precise, scientific procedures which are designed to maintain the integrity of the evidence and to recover "hidden," erased, compressed, encrypted, or password-protected data. Computer hardware and storage devices may contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Since computer data is particularly vulnerable to inadvertent or intentional modification or destruction, a controlled environment, such as a law enforcement laboratory, is essential to conducting a complete and accurate analysis of the equipment and storage devices from which the data will be extracted;

c. The volume of data stored on many computer systems and storage devices will typically be so large that it will be highly impractical to search for data during the execution of the physical search of the premises; and

d. Computer users can attempt to conceal data within computer equipment and storage devices through a number of methods, including the use of innocuous or misleading

filenames and extensions. For example, files with the extension ".jpg" often are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear that the file contains text. Computer users can also attempt to conceal data by using encryption, which means that a password or device, such as a "dongle" or "keycard," is necessary to decrypt the data into readable form. In addition, computer users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography a computer user can conceal text in an image file which cannot be viewed when the image file is opened. Therefore, a substantial amount of time is necessary to extract and sort through data that is concealed or encrypted to determine whether it is contraband, evidence, fruits, or instrumentalities of a crime.

27. Additionally, based upon my training and experience and information relayed to him by agents and others involved in the forensic examination of computers, I know that routers, modems, and network equipment used to connect computers to the Internet often provide valuable evidence of, and are instrumentalities of, a crime. This is equally true of so-called "wireless routers," which create localized networks that allow individuals to connect to the Internet wirelessly. Though wireless networks may be "secured" (in that they require an individual to enter an alphanumeric key or password before gaining access to the network) or "unsecured" (in that an individual may access the wireless network without a key or password), wireless routers for both secured and unsecured wireless networks may yield significant evidence of, or serve as instrumentalities of, a crime—including, for example, serving as the instrument through which the perpetrator of the Internet-based crime connected to the Internet and, potentially, containing

logging information regarding the time and date of a perpetrator's network activity as well as identifying information for the specific device(s) the perpetrator used to access the network. Moreover, I know that individuals who have set up either a secured or unsecured wireless network in their residence are often among the primary users of that wireless network.

28. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrants, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

29. Because several people share the SUBJECT PREMISES as a residence, it is possible that the SUBJECT PREMISES will contain storage media that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless determined that that it is possible that the things described in this warrant could be found on any of those computers or storage media, the warrant applied for would permit the seizure and review of those items as well.

## CONCLUSION

30. Based on the foregoing, there is probable cause to believe that the federal criminal statutes cited herein have been violated, and that the contraband, property, evidence, fruits and instrumentalities of these offenses, more fully described in Attachment B, are located at the locations described in Attachment A. I respectfully request that this Court issue a search warrant

for the locations described in Attachment A, authorizing the seizure and search of the items described in Attachment B.

31. I am aware that the recovery of data by a computer forensic analyst takes significant time; much the way recovery of narcotics must later be forensically evaluated in a lab; digital evidence will also undergo a similar process. For this reason, the "return" inventory will contain a list of only the tangible items recovered from the premises. Unless otherwise ordered by the Court, the return will not include evidence later examined by a forensic analyst.

Dustin L. Carder
Special Agent
Homeland Security Investigations

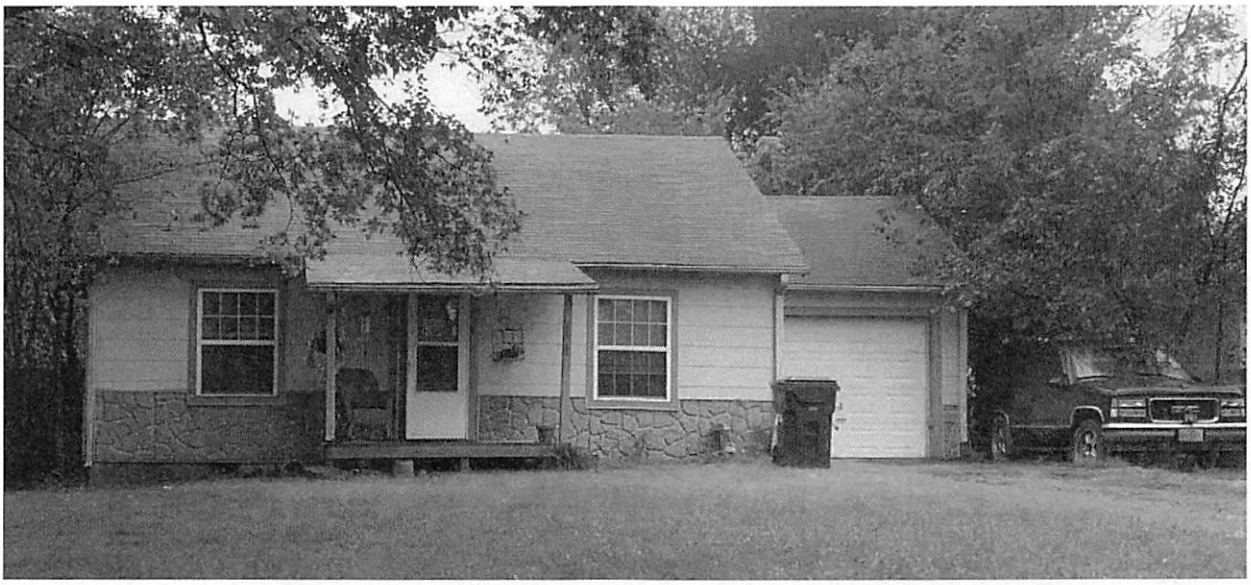
Sworn and subscribed before me this 5th day of ~~October~~ NOV, 2019.

Jodi F. Jayne
UNITED STATES MAGISTRATE JUDGE

# ATTACHMENT A

## DESCRIPTION OF LOCATIONS TO BE SEARCHED

The entire property located at **1403 Archer Drive, Claremore, Oklahoma**, including the residential building, any outbuildings, and any appurtenances thereto (the SUBJECT PREMISES). The residence to be searched is a single-family dwelling with white siding and tan rock along the base, tan trim and a brown composite roof. The front door of the residence to be searched faces north. There is a small overhang covering a porch by the front door with a tan pillar on either side. There is an attached one car garage on the west end of the residence to be searched with a white overhead door. The residence to be searched is described above and pictured below:



## ATTACHMENT B

## LIST OF ITEMS TO BE SEIZED

A. Images of child pornography or child erotica; files containing images; and data of any type relating to the sexual exploitation of minors, and material related to the possession thereof, in any form wherever it may be stored or found including, but not limited to:

* i. Any cellular telephone, smartphone, tablet, personal digital assistant, computer, computer system and related peripherals; computer hardware; computer software; tapes, cassettes, cartridges, streaming tape, commercial software and hardware, computer disks, disk drives, monitors, computer printers, modems, tape drives, disk application programs, data disks, system disk operating systems, magnetic media floppy disks, hardware and software operating manuals, tape systems and hard drive and other computer related operation equipment, digital cameras, scanners, monitors, printers, external storage devices, routers, modems, computer photographs, Graphic Interchange formats and/or photographs, undeveloped photographic film, slides, and other visual depictions of such Graphic Interchange formats (including, but not limited to, JPG, GIF, TIF, AVI, and MPEG), and any electronic data storage devices including, but not limited to hardware, software, diskettes, backup tapes, CD-ROMS, DVD, Flash memory devices, and other storage mediums; any input/output peripheral devices, including but not limited to computer passwords and data security devices and computer-related documentation, and any hardware/software manuals related to or used to: visually depict child pornography; contain information pertaining to the interest in child pornography; and/or distribute, receive, or possess child pornography, or information pertaining to an interest in child pornography, or information pertaining to an interest in child pornography;

ii. Books and magazines containing visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256 or relating to the sexual exploitation of minors;

iii. Originals, copies, and negatives of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256 or relating to the sexual exploitation of minors; and

iv. Stories, text-based files, motion pictures, films, videos, and other recordings of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256 or relating to the sexual exploitation of minors;

B. Information, correspondence, records, documents or other materials pertaining to the possession, receipt or distribution of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256, or pertaining to the sexual exploitation of minors, that were transmitted or received using computer, cellular device, personal digital

* Officers may seize only those cellular telephones that officers reasonably believe are owned or controlled by individuals that reside at the subject premises. JJ 11-5-19

assistant, or some other facility or means of interstate or foreign commerce, common carrier, or the U.S. mail including, but not limited to:

i. Envelopes, letters, and other correspondence including, but not limited to, electronic mail, chat logs, and electronic messages, establishing possession, access to, or transmission through interstate or foreign commerce, including by United States mail or by computer, of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256 or relating to the sexual exploitation of minors; and

ii. Books, ledgers, and records bearing on the production, reproduction, receipt, shipment, orders, requests, trades, purchases, or transactions of any kind involving the transmission through interstate or foreign commerce including by United States mail or by computer of any visual depiction of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256 or relating to the sexual exploitation of minors;

iii. Any and all records, documents, or materials, including any and all address books, mailing lists, supplier lists, mailing address labels, and any and all documents and records pertaining to the preparation, purchase, and acquisition of names or lists of names to be used in connection with the purchase, sale, trade, or transmission, through interstate commerce including by United States mail or by computer, any visual depiction of a minor engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256 or relating to the sexual exploitation of minors;

iv. Any and all records, documents, or materials, including any and all address books, names, and lists of names and addresses of minors visually depicted while engaging in sexually explicit conduct, defined in Title 18, United States Code, Section 2256; or relating to the sexual exploitation of minors;

v. Any and all records of Internet usage including user names and e-mail addresses and identities assumed for the purposes of communication on the Internet. These records may include billing and subscriber records, chat room logs, e-mail messages, and include electronic files in a computer and on other data storage mediums, including CDs or DVDs;

vi. Any physical keys, encryption devices, dongles and similar physical items necessary to access computer equipment, storage devices or data;

vii. Any passwords, password files, test keys, encryption codes or other information necessary to access the computer equipment, storage devices or data; and

viii. Files, records, programs, logs, electronic communications, scanning programs, financial records, hacking software, or router configuration software;

C. Credit card information including but not limited to bills and payment records, including but not limited to records of internet access;

D. Records evidencing occupancy or ownership of the premises described above, including, but not limited to, utility and telephone bills, mail envelopes, or addressed correspondence;

E. Records or other items which evidence ownership or use of computer equipment or any of the devices described in this attachment that are found in the above residence, including, but not limited to, sales receipts, bills for Internet access, and handwritten notes;

F. Any and all adapters, chargers or other hardware items necessary to charge the battery, or to maintain the functioning of, any of the equipment described above; and

G. Any data or materials establishing ownership, use or control of any computer equipment seized from **1403 Archer Drive, Claremore, Oklahoma**.

H. Any and all information, correspondence (including emails), records, documents and /or other materials related to contacts, in whatever form, with minors involving the production, possession and /or distribution of child pornography and the attempt or act of educing, enticing, coercing, or persuading a minor to engage in sexual acts.